REMARKS

Claims 1-10 remain pending in the application, with Claims 1, 3, 6, 7 and 10 being independent claims. Claims 1-10 are again rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Akiyama (U.S. Patent Application Publication No. 2003/0002680 A1).

The Examiner continues to rely on FIGS. 3, 14, and paragraphs 107, 108 and 486 of Akiyama for satisfying all of the recitations of Claims 1-10. Akiyama describes a broadcast reception device and a contact management device using a common master key in a conditional broadcast system. In FIG. 3, Akiyama shows a broadcast station 200 which broadcasts contents information ([Contents}Kch), which is encrypted using a channel key Kch prescribed for each channel, and appending information ([Appending]Km) which contains a terminal ID, a channel key Kch, etc., and encrypted using a master key Km.

In other words, Akiyama describes how the broadcast station 200 broadcasts contents information and appending information, where the contents information and/or the appending information may be encrypted or may contain therein, the channel key Kch, and where the contents information and the appending information are both encrypted using the master key Km. After the contents information and the appending information are encrypted using the master key Km, the contents information and the appending information are broadcast to a reception device.

Once the reception device receives the encrypted contents information and appending information on a particular channel, the reception device decrypts the contents information and appending information using the master key Km, and then determines whether the reception contract for that channel is valid or invalid. If the reception device determines that the reception contract for that channel is valid, the reception device decrypts the contents information of the corresponding channel using the channel key Kch of that channel.

The present invention differs from Akiyama because in the present invention, a security deciphering apparatus is provided for enciphered data transmitted over a public network and a security method using the same. As shown in FIG. 1, a data service providing apparatus 100 in accordance with the present invention communicates with a communication terminal 200.

The data service providing apparatus 100 includes a control unit 110, a database 120, a database 130, a transmitting/receiving unit 140, an enciphering unit 150, and an enciphering unit 160. The database 130 stores hidden security keys Kh, the enciphering unit 150 is used for data M, and the enciphering unit 160 is used for a cipher key Ks.

The communication terminal 200 includes a control unit 210, a key input unit 230, a display unit 250, a memory 270, a transmitting unit 290, a receiving unit 330, a duplexer 310, a voice processing unit 350, and a voice storing unit 370, in addition to the deciphering module 400. As shown in FIG. 4, the deciphering module 400 includes a personal secret key (Kp) storing unit 410, a hidden secret key (Kh) storing unit 430, a first decoding unit 450, a cipher key (Ks) storing unit 470, and a second decoding unit 490.

When the control unit 110 of the data service providing apparatus 100 determines that a data request signal is received, the control unit 110 reads out the data M meeting the data request from the M database 120, and then controls the M enciphering unit 150 in order to encipher the read-out data M by a predetermined cipher key Ks. The control unit 120 reads out, from the Kh database 130, a hidden secret key Kh corresponding to the intrinsic ID information of the security deciphering module 400 included in the communication terminal 200, and then controls the Ks enciphering unit 160 in order to encipher the cipher key Ks used to encipher the data M.

The control unit 110 then controls the transmitting/receiving unit 140 in order to transmit the enciphered data {M}Ks and personal secret key {Ks}Kh to the communication terminal via the public network 50.

The control unit 210 of the communication terminal 200 receives the enciphered data {M}Ks and the personal secret key {Ks}Kh transmitted from the data service providing apparatus 100. When the control unit 210 determines that the personal secret key {Ks}Kh is received, the control unit 210 stores the personal secret key {Ks}Kh in the Kp storing unit 410. The first decoding unit 450 then decodes the personal secret key {Ks}Kh stored in the Kp storing unit 410, using the hidden secret key Kh stored in the Kh storing unit 430, thereby generating decoded data, that is, a cipher key Ks. The cipher key Ks generated from the first decoding unit 450 is stored in the Ks storing unit 470.

When the control unit 210 determines that enciphered data {M}Ks is received from the data service providing apparatus 100, the second decoding unit 490 decodes the enciphered data {M}Ks, using the cipher key Ks stored in the Ks storing unit 470, thereby generating decoded data, that is, data M. The control unit 210 outputs the data M to the display unit and/or voice processing unit in accordance with the type of data M.

The present invention provides improvements in data security over prior art such as Akiyama because, as described above, the cipher key Ks used to encipher the data M requested by a communication terminal can only be obtained by decoding the personal secret key {Ks}Kh generated in accordance with an enciphering operation of the Ks enciphering unit, by using the hidden secret key Kh instrinsically assigned to the communication terminal. Accordingly, although enciphered data is circulated over public networks, its original data can be secured.

Akiyama nowhere suggests these aspects of the present invention.

More particularly, the Examiner has failed to establish a *prima facie* case of anticipation based on Akiyama because Akiyama fails to discloses a security deciphering apparatus comprising: a hidden secret key storing unit for storing a hidden secret key (Kh) corresponding to intrinsic identification information; a first decoding unit for receiving via a public network a personal secret key ({Ks}Kh), generated by enciphering a cipher key (Ks) by using the hidden secret key (Kh), and decoding the personal secret key ({Ks}Kh) by using the hidden secret key

(Kh), thereby obtaining the cipher key (Ks); and a second decoding unit for receiving via the public network enciphered data ({M}Ks), generated by enciphering data (M) by using the cipher key (Ks), and decoding the enciphered data ({M}Ks) by using the cipher key (Ks), thereby obtaining the data (M), as recited in independent Claim 1 and similarly recited in independent Claims 3, 6, 7 and 10 .

Accordingly, independent Claims 1, 3, 6, 7 and 10 are allowable over Akiyama.

While not conceding the patentability of the dependent claims, *per se*, Claims 2, 4, 5, 8 and 9 are also allowable for at least the above reasons.

Accordingly, all of the claims pending in the Application, namely, Claims 1-10, are believed to be in condition for allowance. Early and favorable action is respectfully requested. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicant's attorney at the number given below.

Respectfully submitted,

Paul J. Farrell
Reg. No. 33,494
Attorney for Applicant

THE FARRELL LAW FIRM
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
Tel: (516) 228-3565
Fax: (516) 228-8475

PJF/TCS/dr